WARNING!
The views expressed in FMSO publications and reports are those of the authors and do not necessarily represent the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

The Russian View Of Information War

Mr. Timothy L. Thomas
Foreign Military Studies Office, Fort Leavenworth, KS.

This article was first published in
The Russian Armed Forces at the Dawn of the Millenium,
7-9 February 2000.

INTRODUCTION

This article highlights four basic aspects of Russian information warfare (IW) thinking: terminology and theory; military-technical and information-psychological developments; implications of IO for Russia (and the West); and the impact of IO on military doctrine and national security policy. The article begins with an explanation of the importance of information security issues to 21st century Russia.

THE GROWING ROLE OF INFORMATION IN RUSSIA

On July 25 1999, the *London Sunday Times* reported that American officials believe Russia may have stolen some of the U.S.'s most sensitive military secrets (including weapons guidance systems and naval intelligence codes) in a concerted espionage offensive. The theft was accomplished using computer hacking techniques and reportedly motivated Deputy Defense Secretary John Hamre to note that "we are in the middle of a cyber war." At the same time, defense journals across America are printing a veritable endless stream of articles about the decrepit state of Russia's armed forces. It cannot house its officers or pay them in a timely and adequate fashion and the armed forces are crime-ridden and underfed, according to these reports. Yet Russia allegedly can successfully attack and access America's most secretive defense files? Why is there such a disparity in the apparent information age capabilities of a country with limited information technological assets and an armed force in a poor state of readiness?

To answer that question succinctly, Russian scientists are making do in the absence of a high technology computer industrial base (and finances, which explains the decrepit state of the armed forces) by relying on the capabilities of a plethora of quality mathematicians and scientists that the country has regularly produced. The computer age, particularly its software aspect, draws on

a particular Soviet and now Russian strength–the ability of Russian scientists to write the programs and compose the algorithms that either stable software, creative programs, or hacking requires, making their abilities so attractive to Russia's Ministry of Defense (MOD). This strength is apparent on the pages of many Russian information journals such as *Questions of Protecting Information, Various Branches of Information Service, Information Technology in Plan and Production,* and *Information Resources of Russia*, among others. The computer age has offered Russia and other economically stressed countries a rare opportunity–to be materially and physically much weaker than other powers in the world yet capable of wreaking havoc with not only the military of stronger powers but also with societal elements in those countries via the talents and creativity of scientists and mathematicians.

Russian thinking about potential uses of the information spectrum began long ago but existed under a cloak of extreme secrecy imposed by the Soviet communist regime. Today, Russian security specialists believe that no issue is more important or more fraught with uncertainty than the current and future information environment. There are several good reasons why this is so. First, the free flowing, cross border exchange of information has offered people and organizations in the former Soviet Union unstructured access to information never before available. This relatively unfettered exchange via media and Internet mediums permits citizens and decision-makers alike a variety of ideological, political, religious, and other information sources from which to choose. Such access was once forbidden by strict internal and external barriers. This access is coming at a time when many Russians are still searching for an ideology or set of principles in which they can find the values and purposes for their very existence. Under such conditions, the mass media, especially television and the press, play a much more important role than ever before.

Second, Russians perceive that information itself has developed into a very important type of national or strategic resource. The "informatization" of society through the computerization of machines sharply influences financial markets, business practices, and even the capabilities of military weapons. In the latter case, information can increase the precision and effectiveness of both traditional (missiles, rockets, etc.) and non-traditional (non-lethal, psychological, etc.) types of munitions. Russians believe that countries that possess "information superiority" may be more inclined than before to employ military force. Military objectives may seem more attainable without significant loss of life and with no apparent ecological risk to such countries. Many Russians believe that the recent NATO intervention in Kosovo was based on the dictate of information superiority, thereby virtually guaranteeing a NATO victory.

Third, many Russians believe that a single global "information space" is emerging, which could allow a country to exploit this space and alter the global balance of power. Specifically, a country can dominate in either an important military-political or military-technical competitive realm, or simply deny another country from doing so.

Fourth, Russians realize that few legal restraints exist that can regulate information interventions or even attacks. This factor also encourages the growth of concepts such as cyberterrorism, that is the use by terrorists of information means to penetrate or destroy information security systems of banks, military institutions, or vital societal assets (power stations and other infrastructure facilities and systems). Finally, many Russians understand that they are far behind in the global

race for information superiority and are beginning to appreciate/fear the potential consequences of not competing in that race.

The three final reasons most likely prompted recent Russian calls at the United Nations for a world-wide information security policy and to limit the development of information weaponry and operations. From a Russian perspective, information security is a vital national concern and potential state vulnerability. While Russian security specialists do not entirely understand information operations, they cannot ignore them, even in the short term. It is for these reasons that Russia has spent and is still spending considerable time developing an information security doctrine.

Because of these considerations, the subject of information warfare and information operations has become almost as significant and important to Russian military planners as the issue of nuclear proliferation. Russian theorists warned decision-makers not to submit to external forms of coercive information diplomacy. Simultaneously, subcommittees of the State Duma commissioned studies on both information warfare and "psychotronic" warfare, and Kremlin advisors and the security community are studying how information security issues may affect the country's political, technical, economic, and military policies. Some members of the Russian academic community are also engaged in studying the potential impact of information operations.

The analyst E. A. Belaev, a member of the Russian State Technical Commission (under the President of the Russian Federation), believes that the "informatization" [*informatizatsiia*] of society has led to the collection, processing, maintaining, and exchange of information between actors -- people, organizations, and governments -- in the single information space. As Belaev defines them, the most critical information technologies within this space are those that support:

- Governmental and military command and control organs;
- Financial-credit and banking structure;
- Command and control systems of various types of transport, energy, and ecologically dangerous industries (nuclear, chemical, biological, and others); and
- Warning systems for emergency situations and natural disasters.

Any underestimation of the information security of these systems, Belaev argues, could lead to unpredictable political, economic, ecological, and material consequences, and perhaps even turmoil. Therefore, today nations must consider their national information resources as strategic resources, and protect them accordingly, nearly on a par with nuclear resources. In addition, burgeoning access to global information networks such as the Internet only underscore the necessity for protecting information resources from manipulation, corruption, deception, or outright theft. The Internet has become an arena for potential conflict, especially over unauthorized access to databases. [1]

Russians have been writing about information security for years now. One of the best and most complete explanations of the impact of the information age was offered by Rafael Midkhatovich Yusupov in a 1997 article in the journal *Vooruzheniye, Politika, Konversiya*. Yusupov noted that information security now is the basis and foundation of national security for Russia. Information

security includes: information resources; the rights of citizens, legal persons and the state to receive, disseminate and use information and protect confidential information and intellectual property; systems for forming, disseminating and using information resources; and systems for shaping public awareness (world outlook, moral values, moral assessments, socially permissible stereotypes of behavior and mutual relations among people).

Information, as a result, either helps determine or strongly influences the status of economic, defense, social, political and other components of national security. Information is now the chief strategic resource. The infrastructure of the state is formed by telecommunications and computer networks and distributed data and knowledge bases. The processing, creation, distribution, and use of information is a growing sphere of the economy at large. Information technologies (IT), introduced to all other spheres of society such as science, education, military affairs, and so on, causes a cardinal change in the methods of production and in people's world outlook, style, and character. IT has greatly altered their work and living place.

Information space [2] is physical space in which information flows circulate, with circulation understood to mean perception, transmission, storage, processing and use of information, according to Yusupov. Information becomes one of the decisive factors in the development of the individual, society and the state. Information space has two dangers: it can be used to monitor the state's information resources (defined as the immediate product of intellectual activity of the most qualified and creatively active portion of a country's able-bodied population), thus becoming information espionage; and information interaction can destroy or disorganize the information resources of elements of state structures. These effects can be realized in peacetime, especially if critical application systems are affected, thereby distorting or destroying information used for state management or decision-making. Information space has no state boundaries, no institutions to protect state interests such as border or customs checks. The border is transparent to information resources, and one day states may have to regulate the movement of information flows.

The information security problem has created such dilemmas, procedures, and concepts as computer warfare, information warfare (IW), information opposition, information weapons, and information terrorism. IW is "opposition in information space." Information security problems also create a social security problem in the information sense, since the vital interests of social subjects are affected by information technologies (a new area for human rights activists?). This reference is to technologies that can monitor and regulate the information interaction of people (monitoring phones, correspondence, the Internet, creating data bases on people from bank and sales transactions, etc.), and the technologies that can shape public awareness (new mass media technologies, psychotropic weapons, network technologies permitting access to various negative information such as pornography, and modern computer games that can shape a child's awareness).

Thus, there are three ways that information security impacts national security. First is the security of vital state information resources and information systems, counters to which are being actively developed by countries all over the world. Second is the predominance of the information approach as the emerging primary scientific method of solving national security problems. [3] Finally, information can have an impact on a state or person's social awareness by

manipulation of reality or fact, which in turn can have a significant impact on a state's national security decision-makers.

The recent conflict in Kosovo has done little to assuage Russian concerns about the significant role information will play in national security issues on the eve of the 21st Century. In the case of Kosovo, for the first time the U.S. and NATO justified military activities by different geo-strategic principles other than simply national interests. Writing in *Foreign Affairs*, Joseph Nye asked if it is possible to define interests conventionally in the information age, especially in light of humanitarian concerns that, due to the impact of the mass media, divert public attention away from real strategic issues. He summed up his views stating:

The Canadian media guru Marshall McLuhan once prophesied that communications technologies would turn the world into a global village. Instead of a single cosmopolitan community, however, they may have produced a congeries of global villages, each with all the parochial prejudices that the word implies, but with a greater awareness of global inequality... all in the presence of television cameras and the Internet.[4]

Nye noted that the U.S. now has an interest in the use of outer space and cyberspace similar to the interests the British once expressed for freedom of the seas. Notably, both are the channels through which words and ideas pass and democratic principles can be promoted. However, *the same medium of cyberspace is also promoting the advancement of "democratic interests" (such as humanitarian affairs) to the level of a state interest at a startling pace*. The present U. S. administration clearly appears to agree with this assessment based on their justification for the use of force in Kosovo. In summary, Nye added, "a democratic definition of the national interest does not accept the distinction between a morality-based and an interest-based foreign policy." [5] From this it is clear that new geo-political principles are beginning to emerge in response to the influence of information. And it is this interpretation that worries the Russians.

TERMINOLOGY, AND THE ELEMENTS AND THEORY OF IW

Both the U.S. and Russia appear to have developed separate lexicons of information-related terms over the past several years. On the Russian side, one can read about the information component of the armed forces; the information resources of the state; information aggression; information subversion; information capabilities of a side; information war; information conflict; information superiority; and an information exchange, to name only a few. On the U.S. side, the terms information carousel, information assurance, information function, information grid, information differential, and information operations appear to have no Russian equivalent.

While no official (that is, Ministry of Defense [MOD] and government approved) Russian definition of information warfare is available in unclassified form to date, many different Russian organizations have defined IW according to their particular context and viewpoint. As a result, several unofficial definitions are available from a variety of agencies from speeches or articles. Some were developed by analysts, and some by high-ranking members of the various agencies, including the Federal Agency for Government Communications and Information (FAPSI), the military, the Ministry of Foreign Affairs, the External Security Service, and the State Technical Commission.

What makes these definitions distinct is that the Russians are careful not to copy a Western or even specific U.S. understanding of the term, as noted in military analyst V. I. Tsymbal's comments above. In addition, Tsymbal points out, in the Russian Federation the organs of state security (primarily FAPSI, the External Security Service [SVR], and the Federal Security Service [FSB]) are responsible for the accomplishment of IW in the broad definition of the term. Partial confirmation of this fact was recently affirmed by the attempt of the FAPSI to have the State Duma allow it to control the Internet in Russia. FAPSI, comprising the former KGB Eighth Chief Directorate and 16th Directorate that is somewhat of an equivalent to the U.S. National Security Agency (NSA), alleged that the CIA was creating information weapons and combat computer viruses, and therefore control was needed. [6] Now, it appears that the Federal Security Service is responsible for this task.

However, all of these Russian agencies and the military have provided IW definitions that do seem to adhere to a common theme, namely that information warfare is conducted in both peacetime and wartime. In its peacetime use, the term refers to a broader category, the information security of society and the government in the psychological, scientific, cultural, and production aspects, with special emphasis on protecting state information resources and attempting to influence enemy information resources. In its wartime or more narrow use, the term refers to the attainment of superiority or the reduction of uncertainty through the use of information protection and suppression systems, to include command and control, EW, and reconnaissance, and to attempts to disorganize the enemy. A look at the IW definitions of several agencies, commissions, and ministries follows.

The Sluzhba Vneshnik Razvedka (SVR) definition of IW

Information war, according to the head of the external security service (SVR), is a concept that includes establishing control over other states' information resources, deterring the development of information technology in countries which are potential enemies, possibly disrupting or completely putting out of operation information networks and communication systems, and developing information weapons and systems for safeguarding the security of a country's own information structure and information flows.[7]

Of all the definitions of IW, this is perhaps the most impressive for its variety and inclusion of several geo-political issues (deterrence, etc.); and the most deplorable, for it's designs are to establish world hegemony in this area. Disruption of enemy capabilities and development of friendly IW equipment and information weapons is just the opposite of the United Nations definition offered by the Russians in the Fall of 1998. The SVR is the only service that has a clear mission outside of Russia's borders, although FAPSI also shares some of this burden.

Ministry of Foreign Affairs

Perhaps the most authoritative definition, that is from a high ranking official, of Russian IW was offered by Russian Foreign Minister Ivanov. It was far from the most comprehensive, however. In a letter to the General Assembly of the United Nations on 23 September 1998, he defined information war as "actions taken by one country to damage the information resources and

systems of another country while at the same time protecting its own infrastructures." Within his definition is the object of attack as defined by the Russians-- information resources.

It is extremely important to understand what the Russian's mean by an information resource (IR) and its place in the overall understanding of Russian IW thinking. For military IW specialist Admiral (retired) Vladimir Pirumov, an information resource is understood to be

information which is gathered and stored during the development of science, practical human activity and the operation of special organizations or devices for the collection, processing and presentation of information saved magnetically or in any other form which assures its delivery in time and space to its consumers in order to solve scientific, manufacturing or management tasks.[8]

The Academy of Natural Sciences offered a slightly different definition of IR, defining it as "information received in the process of the life of citizens, society and the state, and registered in the form of a document."[9]

It is likely that this definition was purposely left vague and general to incite discussion in the U.N.. It certainly does not go into half the detail as the other operative definitions within Russian security agencies.

Military definitions

The definitions offered by the military are more specific, as expected, and primarily address battlefield IW. Particularly emphasis is placed on command and control, and reconnaissance-strike complexes. However, the military is acutely aware of the potential destructiveness of peacetime IW, and addresses it as well.

Retired Admiral Vladimir Pirumov was one of the most authoritative persons to define the term so far. He is a former instructor of electronic warfare at the General Staff Academy and also former Scientific Advisor to the President of Russia. He defined information warfare as follows:

"Information warfare" is a new form of battle of two or more sides which consists of the goal-oriented use of special means and methods of influencing the enemy's information resource, and also of protecting one's own information resource, in order to achieve assigned goals.[10]

His definition implies that information warfare is an activity that can be carried on in peacetime as well as wartime. For strict wartime scenarios, Pirumov offered a definition of information warfare in operations that aimed at gaining an information advantage on the battlefield:

"Information warfare in operations (combat actions)" is the aggregate of all the coordinated measures and actions of troops conducted according to a single plan in order to gain or maintain an information advantage over the enemy during the preparation or conduct of operations (combat actions). An information advantage assumes that one's own troop and weapon command and control components are informed to a greater degree than are those of the enemy, that they possess more complete, detailed, accurate and timely information than does the enemy, and that the condition and capabilities of one's own command and control system make it possible to actualize this advantage in combat actions of troops (forces).[11]

Pirumov currently is the President of the Academy of Natural Sciences of the Academy of Sciences of Russia. He played a major part in developing a dictionary of geo-political terms sponsored by his organization and edited by Colonel General Valeriy Manilov, the current First Deputy to the Minister of Defense of Russia. The terminology book defined IW as:

An inter or intrastate information struggle that involves methods which damage or completely destroy the information environment of the opposing side. It is an information influence on various spheres of societal and governmental activity, a system of measures to capture the information resources of a state and key positions in the informatization sphere.[12]

Ministry of Defense civilian analyst V. I. Tsymbal, mentioned above, offered both a broad and narrow definition of information war (he preferred the Russian "informatsionnoya voyna", literally information war), noting that:

In the broad sense, information warfare is one of the varieties of the "cold war"- countermeasures between two states implemented mainly in peacetime with respect not only and not so much to the armed forces as much as to the civilian population and the people's public/social awareness, to state administrative systems, production control systems, scientific control, cultural control, etc. It is namely in this sense that the information security of the individual, society, and state is usually understood.

In the narrow sense, information warfare is one of the varieties of military activity/operations/actions (or the immediate preparation for them) and has as its goal the achievement of overwhelming superiority over the enemy in the form of efficiency, completeness, and reliability of information upon its receipt, treatment, and use, and the working out of effective administrative decisions and their purposeful implementation so as to achieve combat superiority (victory) on the basis of this. The waging of information warfare in the narrow sense is the field of responsibility of mainly the ministers of defense of modern states.[13]

A final definition is offered by Colonel S. A. Komov, a Candidate of Technical Sciences and Professor. Komov wrote more about the topic of IW on the pages of *Military Thought* in the mid ‘90s than any other analyst to date. He defines information warfare within the confines of one of those articles that looked only at its wartime use, defining it as:

...a complex of information support, information countermeasures, and information defense measures, taken according to a single design and planning, and aimed at gaining and holding information superiority over an enemy while launching and conducting a military action/battle. Interconnections between information warfare and other types of operational/combat support and activities that make up its contents should be noted as well (intelligence, information gathering, communications, etc).[14]

Komov believes four issues are at stake in his definition: first, identifying a set of measures to gain information on the opponent and on the condition of an engagement (electronic, weather, engineer, etc,), to gather information on friendly forces, and to process and exchange information between command and control echelons or sites; second, identifying measures to block the

information gathering processes of others, and to feed deceptive information at all stages; third, identify friendly countermeasures; and finally, gain information superiority over the enemy.

An information weapon is another term defined by the Russians. It is a specially selected piece of information capable of causing changes in the information processes of information systems (physical, biological, social, etc.) according to the intent of the entity using the weapon. Information weapons not only are aimed at hardware and software systems as listed below, but also at wetware or the mind. Such latter weapons include acoustic weapons, drugs light electromagnetic weapons and other non-lethals.

Elements of IW

Theorists differ over the elements that comprise IW. Listed here are two variants. Both are products or thinking of either theorists or practitioners who could be considered as Russian info warriors. First, former First Deputy Minister of Defense and former National Security Chief Andrei Kokoshin, who was ultimately responsible for research and development of these information systems, divided information warfare into the following five subcategories:

- Electronic warfare;
- Intelligence;
- Communications;
- Operational command and control systems and;
- Facilities for the protection of command and control systems against enemy influence.[15]

Second, according to civilian Russian MOD analyst V.I. Tsymbal, there are additional categories. Information warfare, in his view, must be considered as an integrated whole of systems working together that includes the following 8 subcategories:

- Intelligence and counterintelligence gathering;
- Maskirovka and disinformation;
- Use of EW systems;
- Debilitation of communications and scrambling of enemy data;
- Determination of to which state a military objective belongs;
- Destruction of an enemy's navigational support;
- Use of psychological pressure on the enemy, and;
- Destruction of enemy computer nets and software programs.[16]

General Theory of IW

General Major N. A. Kostin, Chairman of the Radio-Electronic Department, General Staff Academy, wrote a general theory of IW. He defined IW (he listed both informatsionnoy bor'boy and protivoborstvom as ways to say IW) simply, in accordance with the definition offered at the U.N., as "a form of struggle between sides that involves the use of special methods and means for impacting the information medium of the opposing side and protecting one's own side in order to achieve the assigned tasks." The goal thus is to provide information security for one's own side and lower the information security posture of the opposing side. He noted that the

battle over information is now so important that the battle for ore, oil and markets could fade in comparison. Kostin added that the information struggle is a special category of war because it is an independent type of war, a component element of any other form of war, and it is waged constantly in peacetime and wartime.

Kostin believes that political factors have the greatest impact on the substance of IW, and drive its goals, tasks, and issues. Political factors also determine the means, methods, and characteristics of conducting the battle, its scope and duration, and provide the necessary material support and financial resources. Economic factors determine the scientific and technical development of the computerization of society and the state. Kostin described the information factor as determining the scope of the struggle, the procedure and methods of its conduct, and the capabilities for utilizing them when influencing the enemy's information environment. It depends on the level of computerization of the sides.

The logical elements forming the foundation of IW are categories, laws, patterns, and principles. Categories objectively reflect the essence and core characteristics of the most important manifestations of IW. They represent a body of military-theoretical thought that includes general terms such as information and IW, and particular terms such as protecting information and attacking information. They can reflect the structure, substance, and requirements of IW. The laws of the materialistic dialectic present themselves as well, according to Kostin, as objective laws and patterns of military activity valid for IW. These include the law of the defining role that politics plays in IW, and the laws on the course and outcome of war and IW which depend on economic, socio-political, scientific-technical, and military capabilities. Recognizing patterns that are inherent in IW are where the primary efforts are directed. This includes the pattern of dependency among goals, on the one hand, and available means and capabilities on the other. The effectiveness of IW is determined by the proportionality among the goals, tasks, systems used, and means available, taking into account the enemy's countermeasures.

Russian analysts have developed a methodology to evaluate the effectiveness of the means of counteracting threats to information security. Developed by scientists Vitaliy Nikolayevich Tsygichko, Georgiy Lvovich Smolyan, and Dmitriy Semenovich Chereshkin in 1995, the work builds on the methodological foundation provided by the information security draft. Its goal is to evaluate the effectiveness of an existing information security system and its subsystems, components and elements with the understandable goal of identifying weak points in this system and substantiating the selection of the most rational ways to improve and develop it.[17] This is accomplished through a detailed mathematical modeling process.[18] To date, the U.S. has not succeeded in developing such a coefficient.

The methodology for evaluating the effectiveness of information security consists of eight steps, according to these scientists:

- Defining an information security system;
- Defining the notion of subsystems;
- Classifying subsystems and identifying features of each class;
- Developing conceptual models of the classes of subsystems;

- Determining a set of criteria and formulating a set of problems for evaluating the effectiveness of subsystems;
- Determining a list of normative and variable information necessary for solving effectiveness evaluation problems;
- Developing methods to evaluate the threat to information security as a function of the degree of protection of objects of information security, and developing methods for ranking threats; and
- Developing a practical methodology to evaluate the effectiveness as applied to different classes of information security system subsystems, and performing calculations based on this methodology.[19]

Obtaining this and associated information permits the formulation of the problems for evaluating the effectiveness of existing information security systems, and for posing tasks for creating new information security systems, according to the Russians behind the study.

INFORMATION-PSYCHOLOGICAL/ MILITARY-TECHNICAL ASPECTS OF INFORMATION WARFARE

Information-psychological

Russian military researchers have focused on the informational and psychological stability of individuals and society as a whole for a variety of cogent reasons, but the primary one is the psychological security of Russian citizens. This is due to the striking change that has occurred in the country's dominant ideology, a change that did not occur in the West. Understandably, therefore, the absence of a similar ideological shock has prompted less attention to this subject there. However, more general trends in the West, such as the increased proliferation and use of computer disc driven games and the influence of the Internet on the youth, are impelling increased interest in the subject. Specifically, more American researchers are now pondering the influence of information technology on the minds of its citizens, a phenomenon accelerated by the sort of youth violence that took place in Columbine High School in Littleton, Colorado in April 1999.

The Russian military excels in the study of the impact of the information-psychological aspect of information warfare. To date, the U.S. has not conducted extensive analysis in this area except for those personnel in psychological operations. Conversely, Russia military scientists have been studying not only the ability of information warfare to affect the values, emotions, and beliefs of target audiences (traditional psychological warfare theory), but also methods to affect the objective reasoning process of soldiers. This reminds one of Andrei Kokoshin's 1996 appeal to conduct an in-depth study of the political and social structures of various countries, systems of state control, and "psychological behavioral stereotypes." Instead of relying on massive fires against personnel, weapons, military hardware, and military targets, the "main efforts" should be concentrated in achieving the destruction of the components on which an enemy's capacity for organized resistance depends.[20] That is, Russia is interested in ascertaining how to affect not only the data-processing capability of hardware and software but also the operating principles that drive various cultures, whether they be social or economic. Here the idea of the unwillingness of the U.S. to take massive casualties comes to mind as a behavioral stereotype.

Three books published in the Russian Federation during the last two years serve as an example of this fixation on behavior and on the mind itself. Endorsed by the State Duma's Security Committee, the first book was, appropriately enough, entitled *Informatsionnaya voina* [Information War].[21] This book examined how to manipulate the mind by toying with the algorithms (to include how to model them) that define human behavior. Humans, the author noted, like computers, can have a "virus" inserted in their information system (reasoning process) if the proper algorithms of mental logic can be affected. The authors dubbed this human information virus a "psycho virus," which, according to mathematical formulas, could perhaps be inserted as a "suggestive influence" to alter the mind's algorithms or prevent objective reasoning. The second book, entitled *Psikhotronnoe oruzhie i bezopasnost' rossii* [Psychotronic Weapons and the Security of Russia][22] bore the endorsement of the State Duma's Information Security Committee. It was co-authored by the Chief of the Information Security subsection of the Security Committee of the Duma, Major (retired) Vladimir Lopatin.[23] Lopatin and his co-author, V. D. Tsigankov, defined psychotronics as an inter-disciplinary area of scientific knowledge, which when mediated by consciousness and by perceptual processes, investigates distant (non-contiguous) interactions among living organisms and the environment.

One other 1999 book that handled information-psychological problems was *Secret Weapons of Information Warfare*. The book focused squarely on the psychological impact on the mind by information issues. The chapters of this book are:

1. Basic directions in the Development of IW under Modern Conditions
2. Understanding Phenomenology in Man and Controlling his Behavior. Education on the Use of Psycho-Physical Weapons
3. Methods for the Precise Orientation of Covert Effects on the Human Psyche
4. Psychotronic Means of Subconscious Effects on the Human Psyche
5. The Integral Method of Psycho-Physical Weapons

The psyche is defined in one Russian publication as an active reflection by man of the objective [real] world, the formation of a picture of this world and, based on this picture, self-regulation of one's behavior and activity. The *Secret Weapons* book, plus the *Psychotronic Weapons and the Security of Russia* work by Lopatin and Tsigankov, are part of a series of books known as the "informationization of Russia on the threshold of the 21st century." The important point here is that these three books underscore the Russian belief that informational and psychological matters should be of concern to civilian and military alike as valid subjects for close scrutiny and their effects both positive and negative can be experienced both in peacetime and wartime.

Colonel Igor Panarin of FAPSI, speaking at a conference in 1997, stated that there is a need in Russia to develop information-psychological subunits in government and military directorates. The role of these departments would be to develop strategic and operational measures to prevent or neutralize attempts to control the psyche of Russian society (what he termed the "strategy of psychological defense"). A Main Directorate in Support of Psychological Security would ensure the psychological component of Russian national security.[24]

Methods of persuasion are an IW weapon specifically oriented against the psychological security of individuals. The primary Russian information weapon in this regard is a concept known as

reflexive control (RC), also called "intellectual IW." RC is defined as a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action. There are scientific and mathematical components as well as varied military and technical uses of RC. Komov has noted that the goals of RC are to distract; overload; paralyze; exhaust; deceive; divide; pacify; deter; provoke; suggest; or pressure an opponent with information.

Other less known but reported information-psychological related activities include:

- military unit 10003, which studies the occult and mysticism, reportedly to understand the recruiting and "brain washing" techniques of these groups
- anti-ESP training in the strategic rocket forces, designed to enable missile launchers to establish mental firewalls in case someone from the outside attempts to take over their thoughts
- astrologers in MoD, who predict ambushes, plane crashes, and other phenomenon
- practice with the "25th frame effect," which tries to insert a subliminal message by adding a 25th frame to a movie or computer generated scene (normal viewing is 24 frames a second; the 25th frame, if added, is thought of in the context of a subliminal message)
- applying electromagnetic impulses to the head of a soldier to adjust his/her psychophysical data
- and remote viewing and psychotronics

For example, it has been alleged but never substantiated that during the 1996 Russian elections, a 25th frame was added with President Yeltsin's picture on the night before the elections to some television programming. The intent was to insert a subliminal message into the heads of voters just before the elections. Whether this actually happened or not is not as important as the fact that the idea has life.

Military-technical

On 28 January 2000, Russian President Vladimir Putin announced that Russia would be devoted to sharply increasing the purchase of new weapons and equipment for its armed forces. High-tech conventional weapons were one of his priorities. Called a shift in spending priorities, Putin said the change would involve shifts in priorities by as much as 80% in some categories. [25]

This announcement was predictable based on a recent speech by Marshall Igor Sergeyev, Russia's Minister of Defense, at the end of 1999. The recent war in Kosovo demonstrated to Sergeyev that a new phase of the revolution in military affairs (RMA) is upon us. The US, he noted, demonstrated a significant military-technical breakaway in the sphere of information support of combat operations that must be countered. Putin's changes appear to set in motion a policy designed to provide that counter. Sergeyev's comments, in a December 1999 issue of the military newspaper *Red Star* devoted to military-technical issues on the eve of the 21st century, also discussed the main domestic and foreign threats to Russia, and the main missions and problems of Russia's military-technical policy.[26]

Sergeyev used the term "information" fourteen times in his discussion of military-technical issues. This emphasis is not surprising. Over the past five years, Russian specialists have studied and written about information issues profusely. Some of this effort was reflected in the information aspect of state security, highlighted in both the country's draft military doctrine and approved national security concept.

Sergeyev noted that Kosovo signified the beginning of "contactless", virtual, information-technical warfare. The biggest NATO mil-tech advantage came from information-support systems, such as reconnaissance platforms, which contribute mightily to the US's desire to break away from the rest of the civilized world in such systems. Unable to compete at the present time, Sergeyev believes Russia must look to asymmetric options. The situation is such that

in the coming years, Russia will not be able to support military-strategic and military-technical parity with the leading military powers of the West on a 'symmetrical' basis, especially in the area of non-nuclear armaments...it is necessary to search for a reasonable combination of evolutionary and 'revolutionary' paths and more effective asymmetrical directions for the development of weapons and military technology and technologically outfitting the Russian armed forces.[27]

Sergeyev listed information missions before nuclear and non-nuclear missions in his report, and noted that priority for systems development would go first to information, and then to operational, rear support, and mobility systems. In the field of non-nuclear armaments, Sergeyev placed the highest priority on the development of systems, resources and means for defending government, military and commercial information systems. The goal is to avoid direct mil-tech competition with the most developed countries by creating "asymmetrical" armed conflict means, in which the most vulnerable functional elements of a potential enemy's systems and key target infrastructure are destroyed, thereby devaluing mil-tech superiority.[28]

Sergeyev listed the main weapons and military-technical directions for the armed forces as reconnaissance and command and control, with the latter specifically at the operational-tactical and tactical levels. The goal is to create an integrated information environment, and a single system of military standards to transmit data. Other mil-tech requirements were to equipment universal, information-oriented, and smart; and to make use of miniaturization when possible, and to reduce the wavelength signature of equipment. Both of the latter have heavy information support requirements.

Sergeyev noted the close integration of information systems and nuclear weapons as well. He stated that information-technical developments of both support and defensive systems help guarantee the effective use of nucs, and are a "new aspect of nuclear deterrence." In addition, destructive qualities of weapons based on new physical principles now approach those of nucs. Weapons based on new physical principles signifies a qualitative leap in the forms and means of armed conflict, and changes the parameters of "parity." Russia's main priority in the field of prospective weapons will be guided and electromagnetic energy weapons (with the former highly dependent on information support, the "informatization" of weaponry), cyber- weapons, and stealth unmanned combat platforms, Sergeyev added. At the operational-tactical level, the focus

will be on multi-charge systems, automated reconnaissance-information fields, and precision weapons.

Finally, Sergeyev addressed space needs. Here he called for modern satellites with increased accuracy and longer use, more navigational devices for the soldier, and a new generation of satellites for topogeodesic [29] support to the armed forces.

Sergeyev's concluding remark was that a new phase of the revolution in military affairs has begun and Russian must not lose time. Time frames are such that any further delays in starting a full-scale modernization of the Armed Forces could lead to a fatal, insurmountable advantage to other countries.[30]

Much of the Russian military equipment under development now and reported in the Russian and Western press appears to stick closely to these goals and missions that Sergeyev enumerated. It is doubtful if these systems will be as high-tech dominant as comparable pieces of equipment in the West, but the Russian military-industrial complex is making progress. Systems currently under development and in the process of fielding include the Shkval, the M-55, X-101, X-555, the Iskander, and the Pchela, all of which are examined below. Each is highly dependent on information technologies.

With regard to reconnaissance assets, Russia is also at work on a high-altitude reconnaissance plane that will enable it to acquire real-time targets in local conflicts. Dubbed the M-55, the plane will be able to provide instant targeting for other aircraft and ground weaponry systems, and can download reconnaissance data, including map information, to command facilities.[31] Another reconnaissance system is the UAV known as the Pchela. Operated primarily by the airborne, according to press reports, two Pchela's can be launched every 30 minutes but only two can be controlled at any one time. The current plan is to upgrade this UAV from a reconnaissance to a reconnaissance-and-attack vehicle. Efforts are underway to make the drone all-weather with night sensors, and to improve its TV's resolution. Flight endurance at the present is only two hours.[32]

In 1999 there were several military-technical improvements of note. The biggest headlines were grabbed by Academician Nikolai Guschchin, chief constructor of the Machine-Building Design Office for his development of the Iskander-E missile complex for ground forces. It is designed to accurately hit small-size and pin-point targets. Iskander-E was preceded by Gushchin's Tochka, Oka, and Tochka-V missile complexes. For these achievements Guschchin was named the Russian Biography Institute "man of the year."[33] Russia will also start serial production of the X-101 and X-555 strategic cruise missiles. The X-101 reportedly can hit targets up to 5,000 kilometers away with a 5-6 meter accuracy deviation. Both missiles also have a reduced visibility to radar which makes their detection very difficult.[34]

In the wake of the conflict in Kosovo, Russia is trying to expand exports of its S-400 surface-to-air missile (SAM) system. Its claimed maximum engagement range is 400 kilometers. In addition, Russia is offering a new, integrated command and control system known as the 45L61. The system is designed to control air defense systems, interceptors, and airborne warning and control systems over a very broad area. The export version is known as the Universal-1E, and it

is being offered to CIS countries and perhaps China and India. The system can detect, identify and track airborne targets within a range of 3200 kilometers, flying at a speed of up to 6,000 kilometers per hour, and at altitudes of up to 100 kilometers, according to Russian sources.[35] Such military-technical developments as the Pchela, the Iskandler, and new command and control systems support the demands of Lieutenant General Igor Rogov, First Deputy Chief of Armaments of the Russian Armed Forces, who noted that local wars would require the modernization of existing of modern weapons, and that

These operations are certainly possible only with full military-technical superiority over the enemy that has been achieved first and foremost through the effective employment of long-rang precision-guided munitions that function in the outline of a reconnaissance-strike system with space reconnaissance, communications, navigation, and command and control elements.[36]

The Russian Navy is selling supersonic anti-ship missiles to Boeing, the Kh-31A missile (NATO designation, Krypton). Over a five year period, Russia will sell the U.S. 100 of these missiles. The Kh-31A flies at Mach 4.5 while its closest Russian twin, the Sunburn, which the Russians sold to the Chinese, flies at Mach 3. Some believe Russia is being very clever here, selling a system to China, a counter to the U.S., and then the next generation Sunburn to the Chinese.[37] China and Russia, according to a British newspaper, are developing a long-range missile with a "ram jet" propulsion system that gives the missile a 50 mile range and a speed of Mach 3. Unlike traditional air-to-air missiles with only six seconds of thrust, the "ram jet" has a full minute of thrust. This is reportedly three years ahead of any similar class RAF missile.[38]

In November 1999, the Russian Navy announced the development of the "Shkval", and an export version known as "Shkval-E." Capable of moving at up to 200 knots, the missile is programmed by feeding speed, distance and vector parameters into the missile's automatic pilot. The missile does not have a homing warhead but rather follows a computer-generated program, and is thus very difficult to throw off target.[39]

An interesting source of information on Russia's information warfare capabilities is the journal *Military Parade*. In a May 1996 article entitled "Information Warfare Facilities," author Yuri Perunov discussed the recent Persian Gulf war and the priority for electronic and information warfare that it demonstrated. He noted that the radios, radio-engineering, radar, television, and infra-red optical reconnaissance facilities located on ships, aircraft and earth satellites provided the U.S. and its allies with real time information on all activities of the Iraqi army.[40]

The struggle for on-line information is becoming important because

...virtually all armament and combat material employ electronics operating over the entire frequency range for target acquisition, transmission of data to control troops, as well as for the direction and control of the destruction means and high-precision weapons, enabling the 'detect-fire-and forget' principle to be realized. [41]

Four tasks of the Russian EW forces are as follows: first, monitor electronic emissions and establish data banks in real time; second, jam enemy electronic means; third, EW equipment can be used to guide precision weapons in to destroy a target; and finally, there is passive jamming

and special techniques that includes stealth armament, chaff, smoke screens and aerosols, among other items. This capability destroys the enemy's information field while preventing the transfer of information for friendly sources to potential enemy weapons. The Russians believe that their EW system also can suppress aircraft reconnaissance, navigation and weapons' control radars, including high-precision ones. [42]

The Russian military industrial complex is busy at work producing information warfare equipment, and publicizing it for purposes of external sales. One pamphlet notes that the 122 MM Grad rocket system now has a rocket (LILIA-2) with built-in interference transmitters that are deliverable to locations of communication means and capable of introducing interference in the SW and FM ranges. The operational life of each transmitter is 60 minutes. [43] In addition, the Russians believe they have developed stealth radars that can detect stealth aircraft (such as the 55Zh6-1 and 1L13-3 radars); jammers such as the Shtora-1 that can protect aviation material from IR homers; the Zoopark-1 reconnaissance complex, allowing for enemy firing positions to be fixed with a high degree of accuracy and quickly; and the Senezh-M1E and Rubezh-Me automated air defense forces control systems.

Information technology based-equipment improvements that Russia hopes will maintain a deterrent capability vis a vis the United States include: improving ICBM's capability to penetrate an ABM defense; developing EW assets that disrupt the functioning of the ABM defense, maintaining a reconnaissance, navigation and communications satellite grouping; improving the system of command and control of Strategic Nuclear Forces to permit optimum structuring of a strike in relation to a particular Ballistic Missile Defense alignment; and placing in service long-range, low-signature strategic cruise missiles. (Kh-101) which existing BMD's cannot intercept. [44] The *Washington Times* reported in June that Russia had resumed testing on a high-altitude weapon that fires off an electromagnetic pulse (EMP). [45] It may be part of Moscow's ongoing anti-satellite weapon development program to attack U.S. satellites, which U.S. Secretary of Defense William Cohen has termed "an infringement on our sovereign rights."[46]

The Chechen War has helped the military-industrial complex, it is reported. According to Valentin Rudenko, an arms trade expert with Moscow's *Military News Agency*, "the war has highlighted the necessity of...developing high-precision weapons that can be used without threatening civilian lives. So the process of modernizing weapons has been intensified."[47] In addition, the war has demonstrated the requirement to update military satellites. These satellites provide targeting data and telecommunications support, and intercept communications not only between Chechen field commanders but also between Chechen rebels and supporters abroad. Satellite imagery support is minimal, since there is only one imagery pass a day over Chechnya.[48] According to Pavel Podvig, military space expert of the Moscow-based Center for Arms Control, Energy and Environmental Studies, the imagery satellite is not capable of maintaining data-link contact with Russian forces. Thus it cannot provide current information on the movement of Chechen rebels.[49] Communications and signal intelligence intercepts are providing much more support than the imagery bird. This force limitation would seem to make satellites a priority procurement concern in the coming years. Zinovii Pak, director of the Russian federal government's ammunition agency, confirmed this fact with reporters on 6 October 1999. He noted that high-precision weaponry and satellites will be procured. [50] A report in early January of this year confirmed the gravity of the situation. It was reported that Russia's

early warning system can detect U.S. ICBM launches only for 17 hours a day. This is because only four of Russia's 21 satellites are still working.[51]

OTHER IW IMPLICATIONS FOR RUSSIA, THE SYSTEMOLOGY OF IW

Perhaps the biggest impact of the information technology revolution has been its impact on military art. Information operations are viewed as a separate and self-sufficient type of conflict; as operations that make the initial period of war extremely uncertain (one doesn't know what preparations were prepared by a potential opponent during peacetime to alter the effectiveness of weapons or the strategic perception of the situation at hand, and thus may not realize that the initial period of war has already started); and as operations that increase the tempo of battle, focusing on continuous attacks designed to blind an opponent by destroying his information operations and achieving information dominance. The new formula for war appears to be "acquire-shoot-jam-move-acquire-shoot-jam-move." No longer is warfare cyclical, but much more linear, according to Russian experts. There are far fewer rest periods between major battles. This will put a premium on logistics and command and control mechanisms.

In Tsymbal's view, the conduct of IW is felt at all three levels of military art: strategic, operational, and tactical. He noted that in peacetime, the goal will be to accumulate information on an enemy while developing and testing one's own IW weapons. Immediately prior to military action, and during military action, IW systems will work to destroy first of all command and control systems of the enemy and any other information systems which receive, store or process information of military significance. Or, an IW operation can be run independently prior to the onset of combat actions of the traditional type. [52] Retired Major General Vorobyev, writing in the June 1997 issue of *Military Thought*, noted that wars of the next century will be highlighted by the information-psychological as much as the information-technical confrontation. He stated that information-psychological opposition, information-psychological operations, and information-psychological pressure are three types of activities to expect. Since the impact of military art was written about extensively in other places, as were some of the other implications of IW, no more topics will be developed at this time.[53]

Within the Russian understanding and concept of military systemology, information is viewed as the "nourishment" that gives life to all elements of the system. This in particular applies to reconnaissance, command and control, support, and strike systems. Information warfare as a system, according to one view, includes three components: information support of the functioning of one's own combat systems; information counteraction against the functioning of the enemy's combat systems; and information protection or defense of one's own combat systems against the informational counteraction of a possible enemy. [54]

Under modern conditions, the skillful use of one's information potential and information resources, including information means and systems, increases the force combat potential many times and the effectiveness of using weapons, combat equipment and combat systems on the whole. At the same time, the vulnerability of command and control systems with respect to deliberate and random activity in the information sphere, including the program support of computer systems, continues to increase. Therefore, it is necessary to protect or defend one's information potential--to protect it everywhere and continually, in peacetime and wartime, not

only from a probable enemy but also against unexpected changes in the current situation--social, economic, and diplomatic conditions--as well as from a lack of skill and/or professionalism on the part of subordinates and chiefs.[55]

While there is a growing interest in military systemology, not only in modeling information warfare but national security in general, there still are some who look at it as not much more than witchcraft. For example, Yuri Orfeyev, writing in *Nezavisimaya Gazeta* in 1996, noted that "all of the so-called 'systems of models of optimum function' are nothing but 'the emperor's new clothes' and are used to justify unproductive activity." [56] His, however, appears to be a minority opinion.

NATIONAL SECURITY DOCUMENTS

Russia's current national security documents reflect an increased concern over information security issues than previous versions. The October 1999 draft military doctrine stated that the exacerbation of the information opposition/confrontation is an important feature of today's international context, a destabilizing factor used to achieve destructive military-political goals and affect current operations and the overall security environment. The draft included information-technological (attacks on computers, nets, infrastructure, etc.) and information-psychological aspects of the external threat to Russia, and stated that the greatest internal threat were actions to disrupt or disorganize the Russian Federation's information infrastructure. Information warfare, the document noted, must be coordinated.

Military-strategic features of the new draft doctrine focused on the features of modern war: indirect strategic operations and means of IW, and the development of a massive information preparation (information blockades, expansion, aggression) operation. Confusing public opinion of certain states and the world community, and achieving superiority in the information sphere in either wartime or during the initial period of war were other important missions. This will elevate information security to a basic military security mission, the draft indicated. Finally, in the realm of information-economic principles, the priority mission remained information support of all missions. This includes science and technology issues, information technology equipment, and resource independence in the development of military products.

Also in October 1999 the Russian Security Council approved the country's Concept of National Security. The concept used the word information 20 times. Various sections of the Concept addressed the country's information security and technology needs. The section "Russia's National Interests" included the following information specific interests: observing the constitutional rights and freedoms of citizens to obtain and use information; developing modern telecommunication technologies; protecting the state information resource against unauthorized access to political, economic, S&T and military information; and preventing the use of information for manipulating the mass consciousness of society. The section "Threats to the Russian Federation's National Security" in the information sphere included: attempts by a number of countries to dominate in the world information space and to crowd Russia out of the foreign and domestic information market; and the development of "information warfare" concepts by a number of states envisaging the creation of means of exerting a dangerous effect on the information spheres of other world countries, means of destroying the normal functioning

of information and telecommunications systems, and means for the safekeeping of information resources or of gaining unauthorized access to them.

Finally, under the section "Ensuring the Russian Federation's National Security" a list of tasks to ensure Russia's national security included: implementing citizens' constitutional rights and freedoms for information activities; improving and protecting the domestic information infrastructure and integrating Russia into the world information domain; and countering the threat of the initiation of opposition in the information sphere.[57]

CONCLUSIONS

For the immediate future, no issue is of more concern to Russian security theorists and planners than the information issue. This should be clear from the discussion above. Several elements should leap out at the reader. First, it is apparent that Russia's approach to IW differs significantly from that of the U.S., particularly in its emphasis on theory, disorganization, and information-psychological subjects. It is also quite clear that each security service has its own unique understanding of IW, and is applying it as it sees fit.

Second, it is clear that Russia is continuing its efforts to develop new technologies to support Defense Minister Sergeyev's vision of the information-technical aspect of IW. Simultaneously, efforts will continue to find a breakthrough in the information-psychological aspect of IW. There will be increased emphasis and focus on asymmetric efforts to counter western advances.

Third, Russia will also continue to try to use the United Nations to examine various aspects of IW, and to slow down progress in the west. The United Nations represent Russia's best opportunity to assemble an international forum against the growing perception of unilateralism on the part of the U.S. in the IW arena.

Finally, Russia has inculcated information security thinking into all of its national security documents, reflecting the growing importance of the subject to the security apparatus in Moscow. This includes documents explaining the national security concept, the military doctrine, and the information-technical aspect of military doctrine. Numerous academies and institutes are also following the impact of the informatization of society on national security issues.

It is now time for the west to make some difficult choices. The difference in approaches between Russia and the west grows daily. In light of this fact it will be interesting to see if the west stops wondering "what" Russia wants from information discussions, and focuses instead on "why" it might be good for both sides to begin talks. Talks over something as mundane as terminology and concepts should be easy to initiate, and they will provide the cornerstone for further discussions. Ignoring the problem of discussions will only exacerbate the issue.

Why should the west engage Russia? Here are a few reasons:

First, the Russian approach is dictated by the logic of the dialectic, which means that it offers a unique way of visualizing and accounting for the use or misuse of information technologies and weapons. Discussion offers Westerners consideration of an asymmetric IW mental logic that,

when compared with Western thinking, promises to offer a new method for thinking outside the box and looking at the same problem.

Second, discussion can help Western analysts understand Russian terminology and perhaps lead to the development of a common IW vocabulary, one with which the West must be familiar if it is to learn how to negotiate over the Russian understanding of the concept. This includes different interpretations of like terms. Russia will be one of the main powers in the U.N. pushing its agenda and familiarity with concepts and terms is vital to U.S. negotiators.

Third, discussion would offer Western analysts to consider Russia's emphasis on different aspects of IW (for example, behavior modification through the generation of algorithmic viruses, etc.) and other information-psychological aspects than the West. Discussion could also focus on some areas discussed much less throughly by U.S. analysts (impact on military art and science, and the principles of war [Russia has13 compared to the U.S.'s 9], for example). There is much to be learned from Russia about these processes.

Fourth, discussion can help prevent misunderstanding Russian spheres of emphasis and concern (and vice versa) which can only lead to miscalculations on the part of U.S. or Russian decision-makers. Talking with Russian IW officials may help avoid future conflict by exposing areas of anxiety or consternation. The actual amount of hysteria among military officials responsible for Russia's national security, which borders on paranoia, is grossly underestimated in the West.

Fifth, discussions with Russians can help lower the threshold of Russia's first use nuclear policy. In order not to be misunderstood, the Russians have stated on several occasions and at all levels that they will respond with nuclear weapons if an IW attack is launched against them. And this in light of the fact that they may not be able to tell with certainty where the attack originated! Of course, it is possible that this is only a bluff on the part of the Russians, because one of their methods to get what they want is to offer a credible threat to a potential enemy. Are we willing to go that far and call a bluff of this nature? Russia in turn may make someone an example. Russia's recent "first use" nuclear policy declaration may have originated from this dilemma. Discussion can only help lower the threshold of this first use policy.

Sixth, it is clear that there is no parity in the collection of material on IW thinking. It was broken long ago, and Russia leads the U.S. and the West by an extensive margin. The West's preoccupation and desire to trumpet its own horn has offered Russia and other countries around the world a veritable treasure house of material to read and analyze, while offering in return a slow trickle of information. Discussions would help level the playing field. A conference in which ten Russians and ten Westerners offered papers would be an excellent way to start this effort. At the present time, they know lots about us and we know precious little about them.

Many critics will offer the opinion that any country developing a program with IW capabilities is not a country with whom the U.S. should be discussing anything. This is a mistake. First, every country is developing some type of IW capability, from terrorists to nation states. While capabilities must be monitored, it is the intent to use this capability that should worry us, and it is here that attention should be focused. Second, it is important to discuss IW matters with other countries to help ease the hysteria that IW has generated in some nations. Hysteria results from

vulnerabilities such as a society that has lost its ideology or the perception that psychological control of a nation via the Internet is possible. Much can be done to alleviate these potential problems by simply discussing concerns and potential areas of conflict. Further, a common lexicon of terms can be produced toward the same purpose. We talk about nuclear issues face to face with our counterparts in nations all over the globe. It is time we start the same process over information security issues well before the first crisis arises and matters get so out of hand that we can't recover without severe losses to our information infrastructure or data banks, and to our stability as a nation.

ENDNOTES

1. E. A. Belaev, â€œInformatsionnaya bezopasnostâ€™ kak globalâ€™naya problemsâ€• [Information Security as a Global Problem], a chapter in, *Globalâ€™nye problemy kak istochnik chrezvychaynykh situatsiy* [Global Problems as a Source of Emergency Situations] (location: URSS, 1998), edited by Iu. L. Vorobâ€™ev, p. 125.BACK

2. Information space is defined by Yusupov as â€œthe sum total of data bases and banks, of the technologies of their management and use, and of information/telecommunications systems and networks functioning on the basis of unified principles and according to general rules ensuring information interaction of organizations and citizens and satisfaction of their information needs.â€• See Rafael Midkhatovich Yusupov, â€œInformation Security is the Foundation of National Security,â€• *Vooruzheniye, Politika, Konversiya*, March-April 1997, No 3-4, pp. 35-38, as translated and downloaded from the FBIS web page on 12 September 1998.BACK

3. Â Ibid.BACK

4. Joseph Nye, â€œRedefining the National Interest,â€• *Foreign Affairs*, Vol. 78, No. 4, p. 26.BACK

5. Ibid., p. 24.BACK

6. â€œFormer KGB Reportedly Tries to Control Internet in Russia,â€• *Russia Reform Monitor*, No. 215, January 10, 1997, American Foreign Policy Council.BACK

7. Vyacheslav Trubnikov, â€œSpectrum of Threats Aimed against Russia is Not Decreasing,â€• Nezavisimoye Voyennoye Obozreniye, 17-23 July 1998, No. 26, p. 8 as translated and downloaded from the FBIS web page on 28 July 1998.BACK

8. From a speech delivered in Brussels in May 1996 by Admiral Pirumov entitled â€œCertain Aspects of Information Warfare,â€• p. 2.BACK

9. Â â€œFrom the Dictionary â€˜Geopolitics and National Security,â€™â€• *Military News Bulletin*, No 10, October 1998, p. 14.BACK

10. Â Ibid.BACK

11. Â Ibid.BACK

12. V. L. Manilov, editor, *Geopolitika i natsionalâ€™naya bezopasnostâ€™(Geo-politics and National Security*), Moscow 1998, p. 37.BACK

13. Tsymbal.BACK

14. S. A. Komov, â€œInformatsionnaya borâ€™ba v sovremennoy boyne: boprosy teoriiâ€• (Information Warfare in Modern War: Theoretical Problems), *Voennaya Myslâ€™ (Military Thought*), May-June 1996, pp. 76-80.BACK

15. Â A. A. Kokoshin, â€œVoenno-politicheskie i ekonomicheskie aspekty reformy vooruzhennykh sil Rossii (Military-political and economic aspects of reform of the Russian armed forces), *Voyennaya Mysl (Military Thought*) No 6, 1996, p. 9.BACK

16. Â V.I.Tsymbal, â€œKontseptsiya â€˜informatsionnoy voynyâ€™â€• (Concept of Information Warfare), talk given at a conference in Moscow in September 1995, p 7.BACK

17. Dmitriy Semenovich Chereshkin, Georgiy Lvovich Smolyan, and Vitaliy Nikolayevich Tsygichko, â€œOtsenka effektivnosti sistem informatsionnoy bezopasnostiâ€• (An Evaluation of the Effectiveness of Information Security Systems), Institut sistemnogo analiza RAN (Systems Analysis Institute of the Russian Academy of Sciences), Moscow 1995 (pamphlet), p 8.BACK

18. The â€œspecific effectiveness of a means of counteracting a specific method of threat realizationâ€• is the central concept and starting norm which permits building a normative base of quantitative evaluations of the functioning effectiveness of information security systems, according to these scientists. Specific effectiveness H(sub i,j,k) of a means of counteraction (SP) is understood to mean the degree of effectiveness of fulfillment by the I-th means of its normative functions D(sub I) for counteracting the j-th method of realization of the k-th threat. For a complete laydown of the mathematics, see the document, pp 13-23.BACK

19. Ibid. To implement this process, other information is required. This includes what the Russians refer to as constant and variable information. Fixed information includes the following items:

- list of possible threats;
- methods of threat implementation;
- means of counteracting each method;
- criteria for the effectiveness of means of counteraction, as well as a list of their functional characteristics;
- evaluation of the effectiveness of means of counteraction as a function of the unit cost of defending any given objective or facility;
- criterion for the extent to which an objective is secure against a threat aggregate;
- criterion for the security of a complex objective/facility which consists of several objectives/facilities;
- and a criterion for the effectiveness of the information security system itself.

Changing information includes:

- characteristics of the objectives (structure, relative value of the information, the features and conditions involved in using an information resource as the given objective operates, etc.);
- the extent to which an objectiveâ€™s effective operation is dependent on the degree of its security (based on each countermeasure);
- normative [regulatory] restrictions on the effectiveness of an objectiveâ€™s operation;
- an array of threats to a specific objective, as well as possible methods of their implementation;
- list of possible means of counteraction actually available to any given objective or facility;
- allocated resources;
- and the structure of the existing information security system.

BACK

20. Andrey Kokoshin, â€œWhat Sort of Army Do We Need: Some Military-Political Propositions of the Reform of the Armed Forces in Russia,â€• *Segodnya*, 7 August 1996, p. 5.BACK

21. S. P. Rastorguev, *Informatsionnaya voina* [Information War], (Moscow: Radio and Communication, 1998).BACK

22. V. D. Tsigankov and V. N. Lopatin, *Psikhotronnoe oruzhie i bezopasnostâ€™ rossii* [Psychotronic Weapons and the Security of Russia], (Moscow: Sinteg, 1999).BACK

23. Even the military has written about the subject of psychotronic weapons in its publications. For example, see I. Chernishev, "Polychat li poveliteli 'zombi' blast' nad mirom," [Can a ruler make 'Zombies' out of the world]", *Orientir* [Orienteer], February 1997, pp. 58-62.BACK

24. I. N. Panarin, "Information-Psychological Support of the National Security of Russia," paper delivered at the conference "The Information Security of Russia," Moscow 1998.BACK

25. Putin Approves Proposal to Update Russian Military," *The Kansas City Star*, 28 January 2000, p. A13.BACK

26. Marshal Igor Sergeyev, comments in *Kraznaiya Zvesda* [*Red Star*], 9 December 1999 (no page given), as translated and downloaded from the FBIS web page on 9 December 1999. All of Sergeyev's comments in the next 8 paragraphs are from this document.BACK

27. Ibid.BACK

28. Ibid.BACK

29. Ibid. Geodesy is a branch of applied mathematics concerned with the determination of the size and shape of the earth and the exact positions of points on its surface and with the description of variations of its gravity field. *Websters Dictionary*, Merriam-Webster, Tenth Edition, 1998, p. 487.BACK

30. Ibid.BACK

31. Simon Saradzhyan, "Russians Try out Spy Plane," *Defense News*, 27 September 1999, p. 16.BACK

32. Simon Saradzhyan, "Moscow Plans Buy of Pchela-Like Tactical UAVs," *Defense News*, 22 November 1999, p. 26.BACK

33. Designer of Russian Missile Weapons Man of the Year," *ITAR-TASS*, Moscow, 27 December 1999.BACK

34. Russian Strategic Aviation to be More Powerful Soon--Experts," *Interfax*, Moscow, 12 December.BACK

35. Simon Saradzhyan, "Russia Offers Up Integrated Command System," *Defense News*, 27 September 1999, p. 32.BACK

36. Igor Rogov, "Equipment and Weapons: Toward Rearming through Moderization," *Armeyskiy Sbornik*, 1 November 1999, pp. 35-40 as downloaded and translated by FBIS on 01/03/2000.BACK

37. David Mulholland and Simon Saradzhyan, "Boeing to Buy Russian Missile for Navy Tests," *Defense News*, October 11 1999, pp 4, 27,.BACK

38. Tim Butcher, "Russia and China are Developing Super Fast Missile," *The London Daily Telegraph*, 3 January 2000, p. 1.BACK

39. Moscow *Interfax*, 1445 GMT, 18 Nov3ember 1999, as translated and downloaded from the FBIS web site on 18 November 1999.BACK

40. Yuri Perunov, "Information Warfare Facilities," *Military Parade*, May-June 1996, pp. 73-75.BACK

41. Ibid., p. 73.BACK

42. Ibid., pp. 73-75.BACK

43. Rosvoorouzhenie (State Corporation for Export and Import of Armament and Military Equipment) handout.BACK

44. Sergey Sokut, "Washington Revives Star Wards Program: Moscow has Beaten off a Diplomatic Assault and Is Prepared for Further Actions," *Nezavisimoye Voyennoye Obozreniye*, No 3 (126), 29 Jan-4 Feb 1999, pp 1, 4 as translated and downloaded from the FBIS web page on 15 February 1999.BACK

45. Bill Gertz and Rowan Scarborough, "Inside the Ring: Russian ASAT," *Washington Times*, 18 June 1999, p. 9.BACK

46. John Donnelly, "Cohen: Attack on U.S. Satellite is Attack on United States," ???, 26 July 1999, p. 2.BACK

47. Judith Matloff, Russia Cranks Up Arms Production, Sales," *Christian Science Monitor*, 29 December 1999, p. 1.BACK

48. *Space News* (Russian publication), 6 December 1999, p. 10.BACK

49. Simon Saradzhyan, "Russia to Emphasize Replenishing Spy Satellite Fleet," *Defense News*, 25 October 1999, p. 6.BACK

50. Ibid.BACK

51. Jonathan S. Landay, "Missile Detection in Russia is Flawed," *The Kansas City Star*, 10 January 2000, p. A-1, A-6.BACK

52. Tsymbal, p. 11, 12.BACK

53. See for example, "Dialectical versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations," Timothy L. Thomas, a talk delivered at the U.S. Army War College in April, 1997.BACK

54. Author's discussion with General-Major (retired) V. D. Riabchuk, Fort Leavenworth, September 1996.BACK

55. Ibid.BACK

56. Yuriy Venaiminovich Orfeyev, "Alchemy Second Edition: Immature Sciences Creating Empire of False Knowledge," *Nezavisimaya Gazeta*, 28 May 1996, p. 6.BACK

57. Russian National Security Concept, *Nezvisimoye Voyennoye Obozreniye*, 26 November 1999, as translated and downloaded from the FBIS Web page on 29 November 1999.BACK